



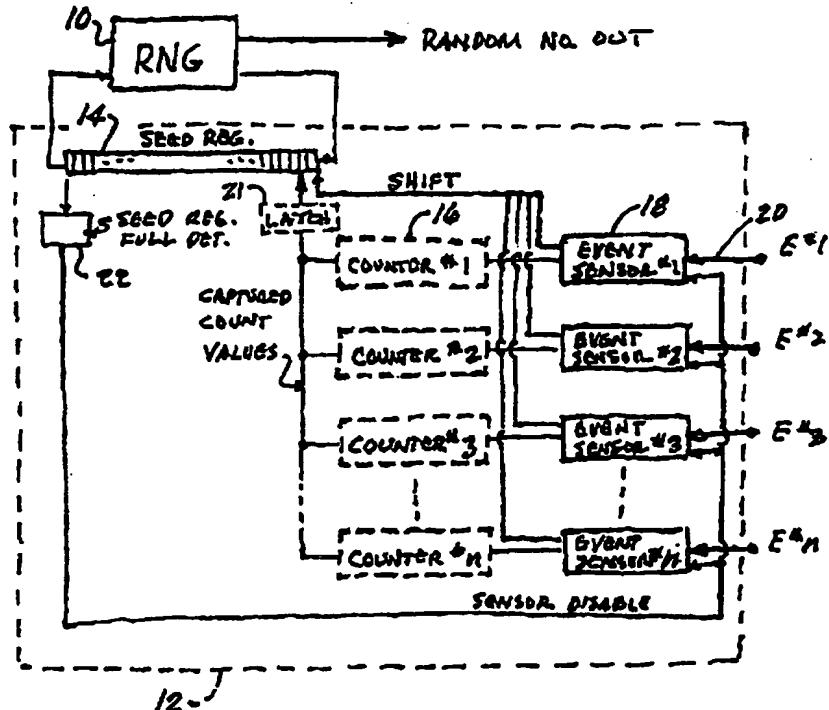
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : G06F 1/02		A1	(11) International Publication Number: WO 00/16182 (43) International Publication Date: 23 March 2000 (23.03.00)
<p>(21) International Application Number: PCT/US99/21105</p> <p>(22) International Filing Date: 14 September 1999 (14.09.99)</p> <p>(30) Priority Data: 60/100,170 14 September 1998 (14.09.98) US</p> <p>(71) Applicant (for all designated States except US): SILICON GAMING-NEVADA, INC. [US/US]; 6685 Amelia Earhart Court, Las Vegas, NV 89119 (US).</p> <p>(72) Inventors; and</p> <p>(75) Inventors/Applicants (for US only): McLOUGHLIN, Bruce [-/US]; 2364 Fatjo Place, Santa Clara, CA 95054 (US). KELLY, John, R. [-/US]; 1024 Summermist Court, San Jose, CA 95122 (US).</p> <p>(74) Agents: HAMRICK, Claude, A., S. et al.; Oppenheimer Wolff & Donnelly LLP, Suite 200, 3373 Hillview Avenue, Palo Alto, CA 94304 (US).</p>		<p>(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).</p> <p>Published With international search report.</p>	

(54) Title: RANDOM NUMBER GENERATOR SEEDING METHOD AND APPARATUS

(57) Abstract

A random number generator (RNG) seeding method and apparatus which includes the provision of an RNG seed register (14) and means for capturing a current count number from one or more fast running counters (16) contained within the apparatus upon the occurrence of an act or acts by an apparatus operator as he performs the normal set-up an initialization function. In the preferred embodiment means (18) are provided for sensing particular acts of the operator (20), and upon detection of each such "event", one or more of the counters within the system are read and the count value is appended to previously captured counters values until the desired seed length is obtained. At this time, the RNG (10) is said to be seeded, the initialization phase is completed and the apparatus may be made available to players to commence game play or other use of the apparatus.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Larvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	VU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		

Specification**RANDOM NUMBER GENERATOR SEEDING METHOD AND APPARATUS**

5

BACKGROUND OF THE INVENTION**Related Applications**

This application claims the benefit of U.S. Provisional Application No. 60/100,170, filed September 14, 1998, entitled "Random Number Generator Seeding".

10

Field of the Invention

The present invention relates generally to random number generator methods and apparatus, and more particularly to an improved method and apparatus for randomly seeding a random-numbered generator.

15

Background of the Invention

In many types of devices, random number generators (RNGs) are used to generate numbers that are used for certain computational purposes, and it is usually important that the starting number or "Seed Value" be truly random because it is this seed value that will determine the sequence of numbers that the RNG will ultimately produce. In one type of application, RNG devices are used in various types of gaming machines including for example, slot machines and similar gambling apparatus, to produce the numbers used to drive the apparatus. See for example, Yfantis, U.S. Patent No. 5,871,400, issued February 16, 1999, and entitled "Random Number Generator For Electronic Applications", expressly incorporated hereinto by reference.

20 Because each machine must operate totally independently of every other machine, the seed value of each machine must be different from that of the others because the seed value will ultimately determine the sequence of numbers that the RNG will produce to drive the game. If two slot machines with the same RNG algorithm are seeded with the same seed value, both machines will produce the same sequence of numbers. This is not permissible because slot machines must

25 include as much randomness as is possible in order to make them "fair" and unpredictable. It is therefore desirable that the RNG seeds for each machine be unknown, unpredictable and different from one machine to another.

30

Before a gaming device such as a slot machine can be put in service, the machine must be initialized. In the usual case, the slot machine goes through at least three phases during initialization; namely, set-up, seeding and finally, the seeded phase, and it is not until the seeded state is reached that a player will be able to use the machine in a normal course of play. The set-up phase is simply a power-on and initialization phase where RAM tests are performed and the various software and hardware modules are initialized. During the seeding phase, a random number is input to the machine, and once loaded, the apparatus is said to be seeded and play can commence. in the prior art various technologies have been used to select a seed value but such value was generated in a way that permitted inspection and the possibility of tampering. There is therefore a need for a method and apparatus that will permit the generation of a seed value that is totally random, unpredictable, and always different from one machine to another.

SUMMARY OF THE INVENTION

An object of the present invention is to provide a novel method and apparatus for generating the seed number to be used in a random number generator.

Another object of the present invention is to provide a method and apparatus for randomly generating and loading a seed number into a register within the random number generator.

Still another object of the present invention is to provide a method and apparatus by which a seed can be randomly generated and loaded into the seed register of an RNG during set-up of the gaming or other apparatus incorporating an RNG.

Briefly, a preferred embodiment of the present invention includes the provision of an RNG seed register and means for capturing a current count number from one or more fast running counters contained within the apparatus upon the occurrence of an act or acts by an apparatus operator as he performs the normal set-up and initialization function. In the preferred embodiment means are provided for sensing particular acts of the operator, and upon detection of each such "event", one or more of the counters within the system are read and the count value is appended to previously captured counter values until the desired seed length is obtained. At this time, the RNG is said to be seeded, the initialization phase is completed and the apparatus may be made available to players to commence game play or other use of the apparatus.

An important advantage of the present invention is that it uses a random sequence and timing of events to obtain a plurality of unknown count values which when captured in sufficient

quantity, will constitute a seed number which is totally unknown, unpredictable and different from one machine to another.

Another advantage of the present invention is that it creates a seeding operation in which it is virtually impossible for the operator to influence the seeding process in a predictable way to 5 obtain a predictable seed number.

These and other objects of the present invention will no doubt become apparent to those skilled in the art after having read the following detailed description of preferred embodiments.

IN THE DRAWINGS

10 Fig. 1 is a block diagram schematically illustrating a first alternative embodiment to the present invention;

Fig. 2 is a block diagram schematically illustrating an alternative embodiment to the present invention; and

15 Fig. 3 is a flow diagram illustrating the operational sequence of the embodiments illustrated in Figs. 1 and 2.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring now to Fig. 1 of the drawing, a first embodiment of a seeding apparatus for an 20 RNG 10 is illustrated at 12 and may be schematically represented as including a seed register in the form of a shift register 14 which loads from the right and shifts left as depicted. Operatively coupled to the input end of register 14 are one or more fast running counters 16 designated 1 through N. These counters are typically not dedicated to the apparatus forming the preferred embodiment of this invention (and are thus shown in dashed lines in Figs. 1 and 2) but are 25 counters used for other purposes in a system including and/or using the RNG 10. It is the ephemeral count per se captured from the counter(s) at one or more particular times ("event times"), that forms an element of the invention. Coupled to each counter 16 is an event sensor 18 which upon sensing the occurrence of an event, as indicated by the input at 20, generates an event signal that causes the current count value of the associated counter to be captured and 30 loaded into register 14, either directly or through an appropriate detecting and latching arrangement (shown in dashed lines at 21). Sensor 18 may also generate a shift signal for causing register 14 to be shifted a number of places corresponding to the number of count value bits input by the corresponding counter 16.

If a single counter and sensor combination are utilized, the captured output of counter number 1 will be sequentially input to register 14 each time event sensor member 1 senses the occurrence of an event (at an "event time") and such action will repeat until a predetermined number of events have been sensed, at which time it is determined that the seed register 14 is 5 full. Alternatively, a seed register full detector 22 may be used to generate a sensor disable signal for disabling sensor number 1. Depending upon the type of RNG utilized, register 14 may offload the entire seed to the RNG, and be zeroed out, or it may form part of several registers or a circulating loop such that the seed continuously circulates through the RNG 10 as part of the random number generating function. At this time, the RNG 10 is said to be seeded and is ready 10 to commence generation of random numbers at its output 24.

In Fig. 2, an alternative embodiment is depicted including an RNG 30, and an associated seed generating circuit is shown in schematic form at 32. As in the previously described embodiment, a register 34 is provided together with a plurality of counters 1-N, as shown at 36, the outputs of which are ganged together so as to simultaneously load the several captured count 15 values in parallel to an input end of register 34 upon the sensing of a particular event by a single event sensor 38. Sensor 38 may also generate a shift command causing the new input to be shifted through the register, and thereby be appended to any previous inputs. The captured count values will be continually shifted through the register 34 each time an event is sensed until either a predetermined number of such events occur, or a seed register full detector 40 indicates a 20 completed seed and perhaps generates a disable signal for disabling event sensor 38. At this time, seed register 34 contains the full seed and is ready to "seed the RNG" 30.

As alternatives to the two above-described implementations, it should be noted that sequential outputs of a single sensor may, on the occurrence of events, be stepped through a plurality of counters to capture and extract the required count values, or the outputs of a plurality 25 of sensors may be similarly applied in order to a single counter upon the occurrence of a series of events to obtain the required count values at the times of occurrences of the events.

Referring now to Fig. 3, a flow diagram is presented in which operation of the above embodiments are generally illustrated in logical operation format. As indicated at block 40, the first step is to turn the system power ON and commence initialization of the system. As 30 suggested by box 42, the power ON operation causes one or more fast running counters to begin counting. As indicated at 44, any current seed value is zeroed out on power up and the system awaits the detection of an operator event as evidenced by b-lock 46. An "operator event" might be the depression of buttons by the operator, the opening of doors, hits applied to a touch screen,

etc., or any other predetermined operator action. Upon the occurrence of the event or events, the current count values of the one or more counters are captured (Block 48). Such value(s) are then appended to any current seed values (values previously captured and collected) as indicated at 50. At this point, the seed is tested to determine whether or not there is a predetermined number 5 of bits in the seed, and if not, the system awaits a subsequent user event and the operation is repeated. However, if the test at 52 indicates that enough bits have been loaded into the seed, the operation will be deemed complete and the RNG will be seeded. At this time the event sensor at step 46 may be disabled and the system made ready for use.

In an actual system, the RNG seed might for example, be a number within the range of 10 600-700 bits. As indicated above, this number is constructed over time using predetermined but "randomly occurring" events that are caused to occur as a result of normal actions taken by a system operator during system initialization. As suggested above, when a particular input event is detected, one or more fast running counters are read. By "fast running" it is meant that the counters are counting at rates fast enough that the operator would have no way of determining 15 what the current count value is at any particular time (e.g. the counters may generate bits in nanosecond units). As the count values are captured, the values are appended to previously counted count values until the desired seed length is obtained. In the particular seeding implementation described, upon each event sensed, the current counts of counters collecting the following statistics are read.

20

Counter No. 1 -- Time Stamp Count (Total Clocks)	27 bits
Counter No. 2 -- Instructions Executed	25 bits
Counter No. 3 -- Date of Reads and Writes	24 bits
Counter No. 4 -- pSOS Microsecond Timer (Time_Get)	<u>20 bits</u>
	96 bits

25

Note that it will take 7 calls to this function to accumulate enough bits to seed a 607-bit FCG and the two 32 bit Marsaglia seeds (total 671 bits) used in this particular system.

Although the present invention has been described above in schematic form, and in terms of several alternative schematic implementations, it will be appreciated that these illustrations 30 are not intended to be exhaustive, and are merely representative and intended to teach one skilled in the art how to implement the invention using his own implementational skills. Moreover, the diagrams are intended to be simple in form and may or may not represent actual implementations of a real system on a one-to-one component basis.

The essence of the invention is that a seed for an RNG mechanism (implemented in hardware, firmware or software) is generated by capturing one or more current count values, typically in digital form, from one or more fast running counters in response to the occurrence of one or more operator acts or caused events. The respective captured values constitute random

5 numbers which when concatenated or otherwise combined, form a larger or different random number for use as a seed. Note that although the captured count values are described above as being shifted into a register, they could alternatively serve as mathematical multipliers or other functions which when used to manipulate other captured or generated values, will yield random numbers of increased complexity. The term "Operator" is used herein to generally represent any

10 human or robotic manipulator that is manipulating system components operating in a non-synchronized relationship to the event counters, or otherwise creating an effect upon or within the apparatus that can be sensed as the occurrence of any event. The term "counter" is intended to include any device or means that changes with time and from which a time related signal can be captured and converted to some type of informational data bits. Examples of such counters

15 might include mechanical or electronic clocks, shaft encoders, timing lights, moving electromagnetic flags, etc., and any sensory detectors associated therewith.

It is therefore intended that the following claims be interpreted broadly so as to cover the full spirit and scope of the invention.

What is claimed is:

CLAIMS

1 1. A method of seeding a random number generator comprising the steps of:
2 sensing an operator induced event;
3 capturing a current value of a fast running counter; and
4 using the captured count value to build a seed value that can be used to seed a
5 random number generator.

1 2. A method as recited in claim 1 wherein the seed value is generated by count values
2 captured from a plurality of counters.

1 3. A method as recited in claim 1 wherein a plurality of event sensors are utilized to initiate
2 the capture of count values.

1 4. A method as recited in claim 3 wherein each counter corresponds to a particular event
2 sensor and outputs a count value in response to an input received from its corresponding sensor.

1 5. A method as recited in claim 1 wherein a plurality of count values obtained from a
2 plurality of counters are simultaneously appended to a current seed value in response to the
3 sensing of a single event.

1 6. A method as recited in claim 1 wherein means are provided for determining when a
2 predetermined number of count value bits have been collected, and for using the collected data
3 bits as a seed for use by the random number generator.

1 7. A method as recited in claim 6 wherein said means for determining that the seed value is
2 complete also disables the events sensor so as to terminate, capture and load of count values into
3 the seed.

1 8. Apparatus for seeding a random number generator in a device using such a generator,
2 said device having at least one fast running counter associated therewith, comprising:
3 at least one sensor for sensing an event and operative to generate a corresponding event
4 signal;

5 at least one detector/latch responsive to said event signal and operative to capture a
6 corresponding current count value of said fast running counter(s); and
7 at least one seed register for receiving the captured current count value and for using such
8 value to build a seed for use by said random number generator.

1 9. Apparatus as recited in claim 8 wherein the seed is generated by count values captured
2 from a plurality of counters.

1 10. Apparatus as recited in claim 8 wherein a plurality of event sensors are utilized to initiate
2 the capture of count values.

1 11. Apparatus as recited in claim 10 wherein each said event sensor corresponds to a
2 particular counter and causes the capture of a present count value in response to the sensing of a
3 particular event.

1 12. Apparatus as recited in claim 8 wherein a plurality of count values are obtained from a
2 plurality of counters, concatenated and simultaneously appended to previously captured count
3 values in response to the sensing of a single event.

1 13. Apparatus as recited in claim 8 wherein said count values are expressed as data bits and
2 means are provided for determining when a predetermined number of count value data bits have
3 been collected and for using the collected data bits as a seed for use by the random number
4 generator.

1 14. Apparatus as recited in claim 13 wherein the means for determining that the
2 predetermined number of data bits has been collected also disables the event sensor so as to
3 terminate capture and load of additional count values into the seed.

1 15. Apparatus for developing a seed for a random number generator in a device using such a
2 generator, said device having at least one fast running counter associated therewith, comprising:
3 means for sensing an event and operative to generate an event signal;
4 means responsive to said event signal and operative to capture a corresponding current
5 count value of at least one fast running counter; and

- 1 means for receiving the captured current count value and for using such count value to
- 2 build a seed for use by said random number generator.

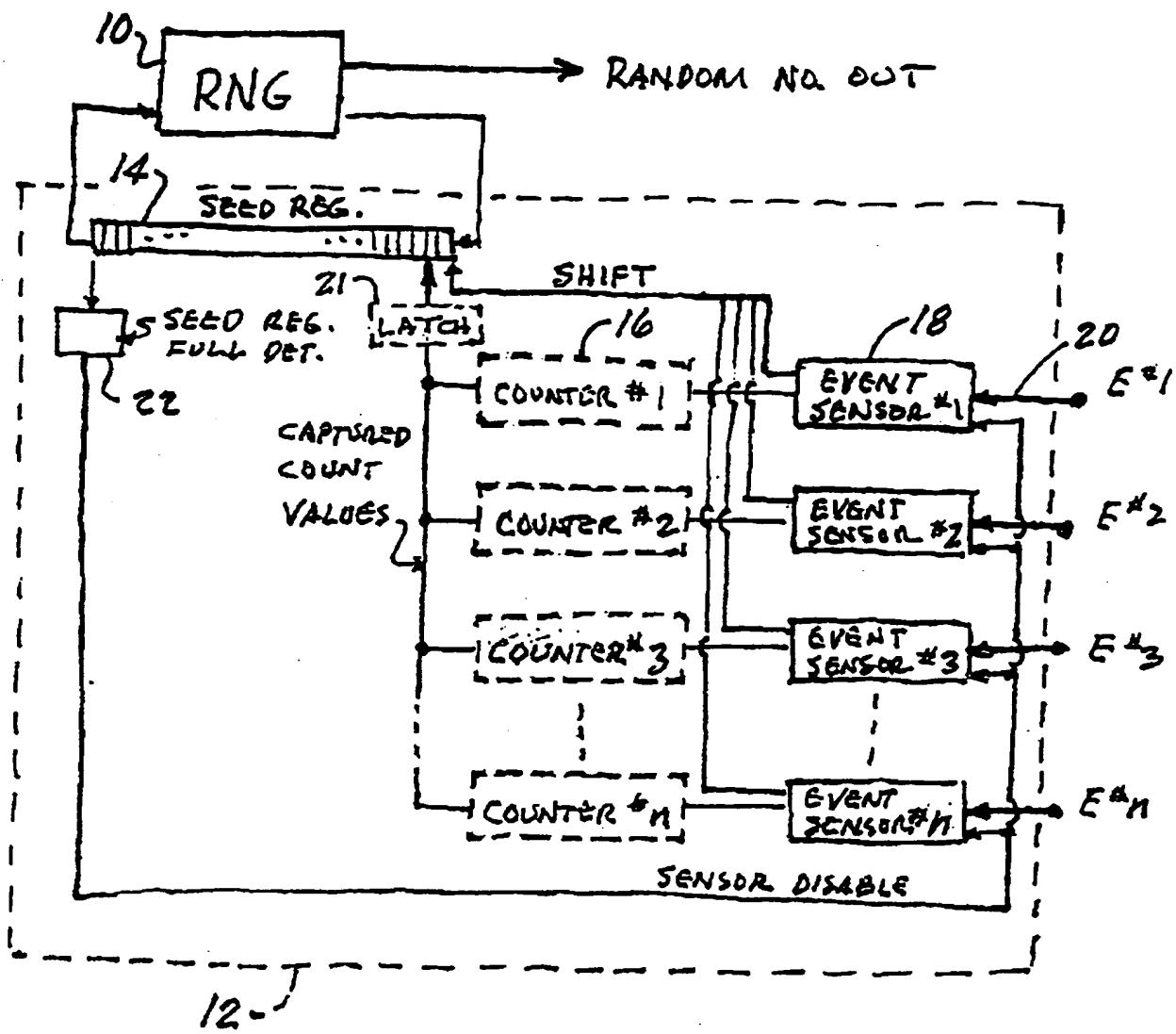


Fig-1

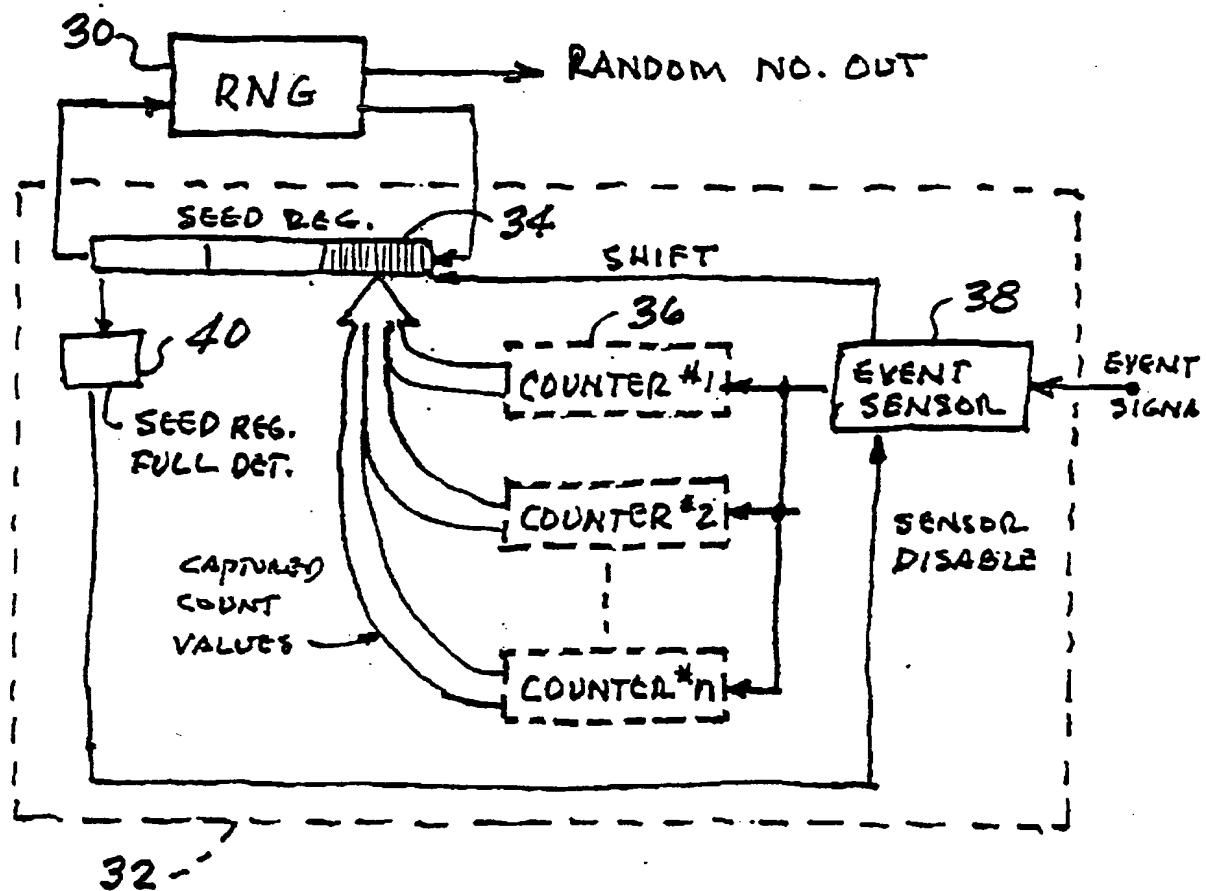


Fig-2

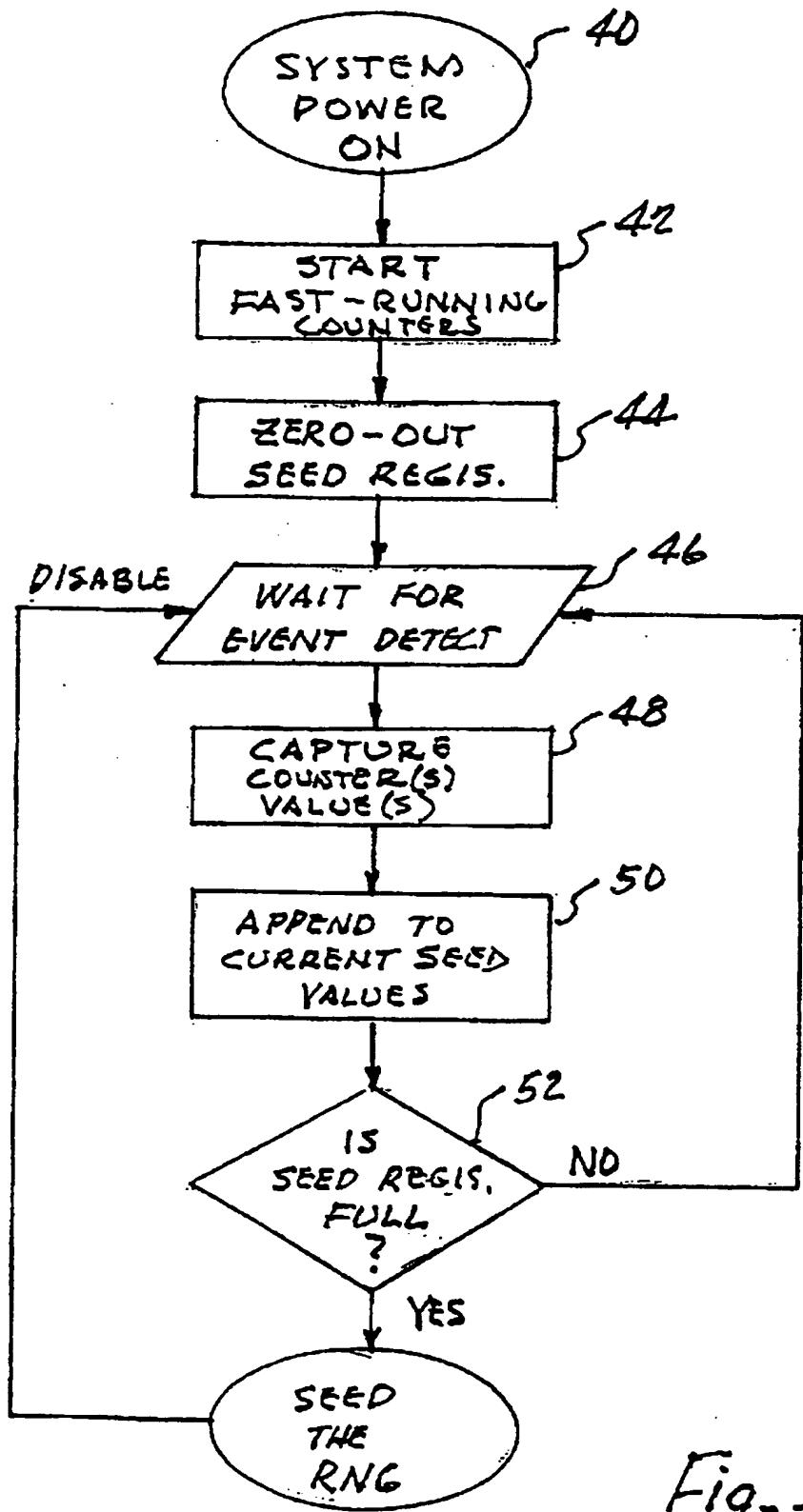


Fig. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/21105

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G06F 1/02

US CL :708/254

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 708/250, 251, 252, 253, 254, 255, 256

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EAST:

search terms: random, seed, counter

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 4,713,787 A (RAPP) 15 December 1987, Figs. 5 & 6.	1-15
A	US 5,383,143 A (CROUCH et al) 17 January 1995, whole patent.	1-15
A	US 5,251,165 A (JAMES, III) 05 October 1993, whole patent.	1-15
A	US 5,463,689 A (SCHUTTE et al) 31 October 1995, whole patent.	1-15

 Further documents are listed in the continuation of Box C. See patent family annex.

Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"		document defining the general state of the art which is not considered to be of particular relevance
"B"		earlier document published on or after the international filing date
"L"		document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reasons (as specified)
"O"		document referring to an oral disclosure, use, exhibition or other means
"P"		document published prior to the international filing date but later than the priority date claimed
"X"		document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step
"Y"		document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is taken alone
"A"		document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
		document member of the same patent family

Date of the actual completion of the international search

26 OCTOBER 1999

Date of mailing of the international search report

13 DEC 1999.

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

CHUONG D. NGO

Telephone No. (703) 305-3800

Jen Hill